Guidelines for Data Protection - Information System Security

The following tables define baseline security controls for protecting Information Systems that store, process or transmit Institutional Data. By definition, an Information System is any electronic system that stores, processes or transmits Institutional Data. This may include workstations, servers, mobile devices (e.g. smart phones, PDAs, etc.) or network devices (e.g. firewalls, routers, etc.). Controls defined in other portions of this document (e.g. Electronic Access Controls, Encryption and Key Management, etc.) also impact the security of Information Systems and should be reviewed to ensure comprehensive implementation of controls.

System Hardening

ID	Control	Public	Private	Restricted
IS-1	Controls are deployed to protect against unauthorized connections to services (e.g. firewalls, proxies, access control lists, etc.)	Required	Required	Required
IS-2	Controls are deployed to protect against malicious code execution(e.g. antivirus, antispyware, etc.)	Required	Required	Required
IS-3	Controls deployed to protect against malicious code execution are kept up to date (e.g. software version, signatures, etc.)	Required	Required	Required

IS-4	Host-based intrusion detection and/or prevention software is deployed and monitored	Recommended	Recommended	Recommended
IS-5	Local accounts that are not being utilized are disabled or removed	Required	Required	Required
IS-6	Default or vendor supplied credentials (e.g. username and password) are changed prior to implementation	Required	Required	Required
IS-7	Services that are not being utilized are disabled or removed	Required	Required	Required
IS-8	Applications that are not being utilized are removed	Recommended	Recommended	Recommended
IS-9	Auto-run for removable Electronic Media (e.g. CDs, DVDs, USB drives, etc.) and network drives is disabled	Required	Required	Required
IS-10	Active sessions are locked after a period of inactivity	Required	Required	Required
IS-	Native security mechanisms are	Recommended	Recommended	Recommended

11	enabled to protect against buffer overflows and other memory based attacks (e.g. address space layout randomization, executable space protection, etc.)			

Vulnerability Management

ID	Control	Public	Private	Restricted
IS-12	Procedures for monitoring for new security vulnerabilities are documented and followed	Required	Required	Required
IS-13	Operating system and software security patches are deployed in a timely manner	Required	Required	Required
IS-14	Mitigating controls are deployed for known security vulnerabilities in situations where a vendor security patch is not available	Required	Required	Required
IS-15	System is periodically tested for security vulnerabilities (e.g. vulnerability scanning, penetration testing, etc.)	Recommended	Recommended	Required

System Logging

ID	Control	Public	Private	Restricted
IS-16	Successful attempts to access Information Systems are logged	Required	Required	Required
IS-17	Failed attempts to access Information Systems are logged	Required for privileged access. Recommended for all other access.	Required for privileged access. Recommended for all other access.	Required
IS-18	Attempts to execute an administrative command are logged *	Recommended	Recommended	Required
IS-19	Changes in access to an Information System are logged	Required	Required	Required
IS-20	Changes to critical system files (e.g. configuration files, executables, etc.) are logged	Recommended	Recommended	Required
IS-	Process accounting is	Recommended	Recommended	Recommended

21	enabled, where available			
IS-22	System logs are reviewed on a periodic basis for security events	Recommended	Recommended	Required
IS-23	System logs are protected against tampering	Required	Required	Required

Supplemental Guidance

IS-18: Administrative commands are those commands that typically require some level of privileged access to execute. For example, adding and deleting users of a system, starting and stopping services and rebooting a system are all examples of administrative commands. Execution of these commands may occur through some type of command-line interface or they may occur through access to a graphical user interface. The full scope of administrative commands that should be logged may vary from one system to the next. As a general rule of thumb, a command that requires the use of sudo on a UNIX or Linux platform would be considered an administrative command. On a Windows platform, a command that requires a typical user to “Run as administrator” would constitute an administrative command.

https://www.cmu.edu/iso/governance/guidelines/data-protection/information-system.html